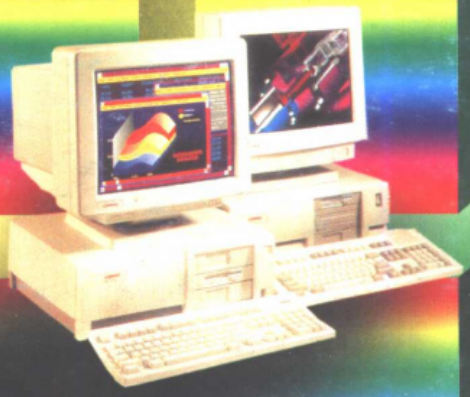
·计算机实用技术操作指南丛书·

计算机防病毒技术指南

本书编委会编写



Personal Computer

北京科学技术出版社

·计算机实用技术操作指南丛书之六·

计算机防病毒技术指南

本书编委会编写

北京科学技术出版社

主　编：陈　凌

编　委：薛　虹　王战峰　张　奎　陶　峰
叶晟翌　刘建军　郭　鹏　朱怀球

目　录

第一章　计算机病毒概述

§1.1　计算机病毒究竟是什么……（1）
§1.2　计算机病毒的产生……（1）
§1.3　怎样确认你的计算机已经感染上了计算机病毒……（2）
1.3.1　效果论方法……（2）
1.3.2　解剖论方法……（3）
1.3.3　比较论方法……（3）
§1.4 发现病毒后怎么办？……（3）

第二章　计算机病毒有关的一些知识

§2.1　软盘……（5）
2.1.1　软盘的结构……（5）
2.1.2　物理扇区和逻辑扇区……（5）
2.1.3　DOS 系统的软盘组织……（6）
§2.2　硬盘……（9）
2.2.1　硬盘的结构……（9）
2.2.2　硬盘的数据组织……（10）
2.2.3　主引导扇区……（10）
2.2.4　DOS 分区和 DOS 引导扇区……（11）
2.2.5　文件分配表(FAT 表)……（11）
2.2.6　根目录表(RDT 表)……（12）
§2.3　DOS 操作系统……（14）
2.3.1　DOS 的基本结构……（14）
2.3.2　DOS 引导程序……（14）
2.3.3　基本输入输出系统(BIOS)……（14）
2.3.4　磁盘操作和文件管理(IBMDOS)……（15）
2.3.5　命令处理程序(COMMAND.COM)……（16）
2.3.6　DOS 软盘启动过程……（16）
2.3.7　DOS 硬盘启动过程……（16）

2.3.8 DOS 的内存分配 …… (17)
§2.4 文件系统 …… (18)
2.4.1 文件系统的目录结构 …… (18)
2.4.2 文件控制块(FCB)、程序段前缀(PSP)、磁盘参数表 …… (18)
2.4.3 .COM 文件和.EXE 文件 …… (20)
§2.5 中断系统 …… (22)
2.5.1 DOS 中断方式 …… (23)
2.5.2 中断向量表 …… (23)
2.5.3 与病毒有关的中断向量 …… (24)

第三章　剖析病毒

§3.1 一个病毒的解剖 …… (27)
§3.2 又一个病毒的解剖(小球病毒) …… (29)
§3.3 计算机病毒的结构 …… (30)
3.3.1 引导模块 …… (30)
3.3.2 传染模块 …… (30)
3.3.3 破坏模块 …… (31)
§3.4 病毒的攻击目标(你的弱点) …… (31)
3.4.1 不要认为它们总是可靠的 …… (31)
3.4.2 直接毁坏 …… (32)
3.4.3 最容易受攻击的文件——活跃的、可执行的文件 …… (33)
3.4.4 关心你的内存(敌人可能已经潜伏了) …… (33)
§3.5 有了病毒以后(简单易行的办法) …… (33)
3.5.1 免除病毒侵害 …… (33)
3.5.2 使用特殊的实用程序 …… (34)
§3.6 计算机病毒的侦测方法及防治技术(程序员水平) …… (35)
3.6.1 病毒的侦测方法 …… (35)
3.6.2 病毒的检测和消除及一些实用技术 …… (38)

第四章　杀毒、防毒软件原理与使用技巧

§4.1 杀毒、防毒软件原理与选用准则 …… (50)
4.1.1 杀毒、防毒软件原理 …… (50)
4.1.2 反病毒系统选用标准 …… (50)
§4.2 KILL 使用技巧 …… (52)

4.2.1 KILL 使用方法 …… (53)
4.2.2 KILL 使用注意要点 …… (54)
§4.3 SCAN 使用技巧 …… (54)
4.3.1 SCAN 命令参数 …… (55)
4.3.2 SCAN 使用要点 …… (57)
4.3.3 SCAN 注意要点 …… (57)
§4.4 CLEAN 使用技巧 …… (58)
4.4.1 CLEAN 命令行参数 …… (58)
4.4.2 CLEAN 使用方法 …… (58)
§4.5 CPAV/MSAV 使用技巧 …… (59)
4.5.1 CPAV 的安装 …… (59)
4.5.2 CPAV/MSAV 简明菜单快速使用 …… (61)
4.5.3 CPAV 全屏幕菜单的使用 …… (64)
4.5.4 CPAV/MSAV 命令行使用方法 …… (72)
4.5.5 CPAV/MSAV 使用技巧和注意要点 …… (75)
§4.6 VSAFE 使用技巧 …… (76)
4.6.1 VSAFE 的启动 …… (76)
4.6.2 VSAFE 的应用 …… (78)
4.6.3 VSAFE 使用注意要点 …… (80)
§4.7 BOOTSAFE 使用技巧 …… (80)
4.7.1 BOOTSAFE 使用方法 …… (81)
4.7.2 BOOTSAFE 使用注意要点 …… (83)
§4.8 NAV 使用指南 …… (83)
4.8.1 NAV 安装方法 …… (84)
4.8.2 NAV 启动方法 …… (84)
4.8.3 选择合适的保护方式 …… (84)
4.8.4 在 Microsoft Windows 下的防毒 …… (85)
4.8.5 在网络上的使用 …… (85)
§4.9 Windows 和网络病毒防治问题 …… (86)
4.9.1 关于 Windows 防毒杀毒问题 …… (86)
4.9.2 NOVELL 等网络防毒杀毒问题 …… (86)
§4.10 防病毒卡操作使用指南 …… (87)
4.10.1 防毒卡开关设置 …… (87)
4.10.2 防毒卡安装 …… (87)
4.10.3 与 TVGA 显示卡兼容问题 …… (87)
4.10.4 对肯定式报警的处理 …… (87)

4.10.5　对疑问式报警的处理 …… (88)
§4.11　防病毒卡的作用和问题 …… (89)
4.11.1　防病毒卡工作原理 …… (89)
4.11.2　防病毒卡特点分析 …… (89)
4.11.3　防病毒卡的问题和评价 …… (90)
4.11.4　选用防病毒卡应考虑的特殊问题 …… (91)
§4.12　杀毒、防毒注意要点…… (91)
附录一　DOS 上一些已知的病毒 …… (93)
附录二　计算机病毒传染后文件增加的字节长度…… (117)
附录三　计算机病毒的特征字…… (120)

第一章　计算机病毒概述

伴随着计算机技术的发展和普及，计算机病毒像生物病毒侵袭人体一样侵袭和威胁着计算机系统。当人们察觉到某种病毒在周围传播，不要多久，这一地区的大多数兼容计算机就会检查到同一种病毒，大量的磁盘被感染，数据被破坏，甚至计算机系统被摧毁等等。计算机病毒悄悄地，快速地传染开，使许多计算机工作人员感到吃惊和困惑。

§1.1　计算机病毒究竟是什么

由于计算机病毒发展早期的隐蔽性，传染的快速性和种类的多样性，往往使人们还来不及给计算机病毒以十分确切的定义。在人们渐渐了解和认识计算机病毒的过程中，许多计算机工作者才从不同的角度给出了计算机病毒的定义，从而帮助人们互相交流，以研究和防治计算机病毒。

我们认为，计算机病毒是一种侵入计算机内部，可以自我繁殖、传播、具有破坏性的计算机程序。

§1.2　计算机病毒的产生

1949 年，计算机的创始人，冯·诺依曼(John Von Neumann)在世界上第一台计算机诞生之后仅仅 4 年，就发表了题为“复杂自动机器的理论和结构”的论文，指出计算机程序可以在内存中进行复制。

1959 年，美国 AT&T Bell 实验室的 3 个年轻人，道格拉斯·麦克尔罗伊(Douglas Mcilry)、维克特·维索特斯基(Vietor Vysotlsky)及罗伯特·莫里斯(Robert Morris)利用公司机器中的核心存储器中的数据和程序来做游戏。他们通过改变磁心存储器中的代码来消毁其它的程序。这种游戏被他们称为“磁心大战”(Core War)．为此，他们设计出有自我复制能力，并在探测到敌方程序运行时能消毁其程序的程序。这个程序经过不断改进，其威力渐渐增大，甚至发展到影响 Xero 530 机的正常运行。意识到这种能 自我复制程序的潜在危险，磁心战被停止了，并在有关人员的默契中保守了这个秘密。

1983 年，弗雷德·科恩(Fred Cohen)博士研制出一种能在运行过程中复制自身的破坏性程序，在全美计算机安全会议上提出并在 VAX/150 机上作了演示。由此证实了计算机病毒的实际存在。

1985 年，IBM PC 机上出现了恶意的特洛依木马程序(Troy Horse)，该程序在显示

漂亮的图象效果的同时，删除磁盘上的文件。

1986 年，在巴基斯坦的拉合尔，一家出售 IBM PC 微机的商店，年青的两兄弟阿姆加德(Amjad)和巴锡特(Basit)，动手编制了一个计算机病毒，并在程序中注明了自己的姓名和地址。这就是所谓的巴基斯坦病毒。

1987 年 5 月，帕金斯·坦尼电脑公司为了防止非法复制其软件产品而制造的病毒在美国普罗威斯顿日报编辑部的计算机上显示信息："欢迎进入土牢，请小心病毒"。

1987 年 12 月，IBM 公司的计算机网络由一份电子邮件传入了"圣诞节蠕虫程序"。每当用户显示内容时，病毒程序就以链方式自我复制，最后导致网络拥挤，使部分计算机被迫停止运行。

1988 年 3 月，潜伏于苹果机中的病毒发作。被广泛感染的苹果机都停止了工作，并显示信息："向所有苹果电脑的使用者宣布世界和平的消息，以此庆祝苹果机的生日。"

1988 年 11 月 2 日，美国康奈尔大学 23 岁的研究生罗伯特·莫里斯(Robert Morris)制造的蠕虫事件，则是一起震撼全世界的计算机病毒侵入网络的案件。这个事件是计算机病毒演化过程中的一个重要转折点。

1989 年 11 月 13 日，星期五，一个被称为"黑色星期五"的恶性病毒在长期潜伏广泛传播后，在全世界数十万台运行 DOS 的微机上发作。这一天，每运行一个文件，则被删除一个文件，许多微机被迫停机，造成的损失难以估计。

§ 1.3 怎样确认你的计算机已经感染上了计算机病毒

如何诊断一台计算机和一个软件是否已经染上了计算机病毒呢？至少有下列三种方法：即效果论，解剖论和比较论方法。

1.3.1 效果论方法

计算机病毒由于是一段具有破坏性的程序，尽管它的执行隐密，却仍可以露出马脚来。表现为：

(1) 机器运行速度明显减慢。

(2) 没有做磁盘读写，却发现磁盘指示灯亮。

(3) 列目录时发现软件的字节数增加。

(4) 病毒软件的自白。例如：屏上显示"Your PC is stoned"，提示有合法大麻病毒；用 DIR 列目录或用 LABEL 查卷标时，见卷标已被改为 Brain，提示有巴基斯坦智囊病毒；屏幕上显示小球作弹性碰撞，提示有小球病毒；奏出一段杨基曲，提示有杨基病毒。

(5) 文件莫名其妙地消失。

病毒的表现常需要一些条件，例如小球病毒在整点或半点，调用 INT13(磁盘 I/O 中断，例如 DIR 就用到这个中断)时开始发作。杨基病毒在下午 5 点整开始奏曲。创造

病毒激活条件(类似于实验室中培养细菌),是诊断计算机病毒的一种效果论方法。

1.3.2　解剖论方法

病毒程序或被感染程序通常具有解剖特征,而且日益发展的软件技术提供了许多能对软件进行外科手术的工具软件,例如:debug,pctool,Norton。举两例如下:

1. 确诊 n 驱是否有小球病毒(n 取 0,1 或 2 分别代表 A,B,C 盘)。

C>debug ↵

—L 100 n,0,1, ↵ {装入 n 号盘,0 扇区}

—U ↵ {反汇编}

如果显示的第一条指令是 JMP 11E,则确诊已染上小球病毒。

2. 确诊 test.com 是否已感染"黑色星期五"。

c>debug test.com ↵

—RCX ↵

CX:8177　　{test.com 和字节数,16 进制}

S 100:L8177"SUMSDOS" {搜察特征串}

XXXX:8171 {在 8171 处找到特征串}

则可确诊已感染"黑色星期五"。

解剖论方法有下列难点:

(1)通常需要用户熟练掌握软件"外科手术"工具,需要较高的技巧,需要关于汇编和机器代码的知识。(2)手术过程交互式操作不能自动化地重复,熟练程序员也难免犯错误。(3)如果不预知病毒特征,则需理解程序代码,由于病毒手段花样百出,需要较高的汇编技巧和实践经验。

1.3.3　比较论方法

首先提取并保存一套重要数据的正确版本,例如不同版本的总引导扇区(分区表)、引导扇区,中断向量表,可执行文件字节数,然后开发一套自动或半自动的检测系统,彻底扫描被查软件的参数,再与正确版本对比,如有异常,则提示已被病毒感染,接着用正确的数据覆盖错误数据,达到消灭病毒的目的。

§1.4　发现病毒后怎么办

试想一下,当你或家人患了感冒你会怎么办?对了,去看医生,或是开点药,依法服下,休息两天,绝大多数的情形是服药之后病情一天天有所好转,如果服了药还不见好,就要去做进一步的检查了。计算机也同理。当你发现你的机器有如 1.3 节所述症状时,首先假设这就是病毒所致,拿出你早已准备好的杀毒软件来(如果没有也有办法,但我建议您最好时刻保有最新版本的杀毒软件),就地施法。

如果杀毒之后，情形依然不变，则先关机，用一张干净的系统软盘重新启动，然后用带有杀毒软件的软盘杀毒。如果依此做过之后，系统依然有问题，就要找专门的电脑诊所了。

其实，消灭病毒最简单的办法就是关机，然后重装一遍系统，将磁盘全部重新格式化。但是，这是我们都不愿意首先使用的下下策了。

在这一章，我们谈及了计算机病毒的定义、产生、发展过程，以及怎样诊断计算机病毒和防治的最普通的方法，下一章我们将详细阐述有关计算机病毒的技术基础以及计算机病毒的作用机制，有兴趣的读者可以继阅读。

第二章　计算机病毒有关的一些知识

上一章我们谈到计算机病毒是一段具有破坏性的程序，它的攻击目标主要是磁盘和文件。这一章我们就先从磁盘和文件系统的结构谈起，然后剖析DOS操作系统，最后破解病毒的作用机制。看完了本章，你将会对所有的基于DOS的病毒有一个彻底的了解，同时也使你更深入地了解你手头的计算机。

§2.1 软　盘

2.1.1 软盘的结构

目前，微机使用最普遍的是5英寸盘和3英寸盘。

软盘有单面，双面之分，也有双密度和高密度之分。但不管是何种软盘，其基本结构是完全类似的。每张软盘由若干条磁道组成，最外面的磁道为0磁道，向内依次为1磁道，2磁道…。格式化之后，每条磁道又分为若干扇区，每个扇区不管其长度大小，都存储512个字节，所以每张磁盘的容量为扇区数和512的乘积。

每个扇区由4部分组成，依次为标识区(ID区)，间隙，数据区(DATA)和间隙。

ID	间隙	DATA	间隙

标识区用来标识扇区的开始和记录目标地址的信息，数据区用来记录数据。两个区之间均留有空隙，以保护数据不受盘速变化、机械尺寸、延时误差等等因素的影响。

2.1.2 物理扇区和逻辑扇区

磁盘的扇区定位可使用两种方式来实现：物理扇区和逻辑扇区。物理扇区是指某个扇区在磁盘上的绝对位置。因而，物理扇区由驱动器号、面号、磁道号、扇区号4个参数组成。驱动器号指磁盘所在驱动器，对应的编号A驱为00，B驱为01，C驱为02，以此类推。在同一张软盘上，第一个物理扇区是0面0道1扇区，而最后一个物理扇区是1面39道9扇区。为了减少磁头移动的次数，磁头在访问磁盘时是从同一道中一个面中的所有扇区，到下面中所有扇区，然后才移动到下一道。以这种顺序访问磁盘是较合理的。

逻辑扇区是将一张盘片上的所有扇区统一顺序编号。这个编号就称为逻辑扇区或"相对扇区"。逻辑扇区以DOS区域起始的物理扇区为逻辑0扇区。对于双面双密度软

盘，为了减少磁头寻道时间，其逻辑扇区的编号从 0 面 0 道 1 扇区为逻辑 0 扇区开始，到 0 面 0 道 9 扇区为逻辑 8 扇区，而 1 面 0 道 1 扇区为逻辑 9 扇区，直到 1 面 0 道 9 扇区为逻辑 17 扇区等等。若用 16 进排列，双面双密度软盘的逻辑扇区号，请看表 2.1。

表 2.1 双面双密度软盘的逻辑扇区号(十六进制)

	0 面									1 面								
扇区 / 道号	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9
0 磁道	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11
1 磁道	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	20	21	22	23
2 磁道	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	30	31	32	33	34	35
3 磁道	36	37	38	39	3A	3B	3C	3D	3E	3F	40	41	42	43	44	45	46	47
⋮	…									…								
38 磁道	2AC	2AD	2AE	2AF	2B0	2B1	2B2	2B3	2B4	2B5	2B6	2B7	2B8	2B9	2BA	2BB	2BC	2BD
39 磁道	2BE	2BF	2C0	2C1	2C2	2C3	2C4	2C5	2C6	2C7	2C8	2C9	2CA	2CB	2CC	2CD	2CE	2CF

逻辑扇区与物理扇区的对应换算关系，可用下列公式表达：

逻辑扇区号=(道号×面数+面号)×每道扇区数+扇区号−1

DOS 系统分配磁盘存储空间的最小单位是簇。一个簇由几个连续的逻辑扇区组成。每个簇中的扇区数与盘的类型和 DOS 的版本有关，一般单面软盘或高密软盘每簇为 1 个扇区，双面双密软盘每簇 2 个扇区。

2.1.3 DOS 系统的软盘组织

DOS 系统格式化的软盘由四个部分组成：引导扇区(Boot Area)、文件分配表(FAT 表)、根目录表(RDT 表)和数据区(Data Area)。

1. 引导扇区(Boot Area)

引导扇区位于逻辑 0 扇区，即软盘片的 0 面 0 道 1 扇区上。由 FORMAT.COM 程序格式化磁盘时形成。引导扇区的主要功能是完成 DOS 的自举。引导扇区由 3 个主要部分组成：

(1) 磁盘基本输入输出参数块；(2)磁盘基数表；(3)引导程序。

在引导扇区的位移 0BH 到 1EH 处，是长度为 19 个字节的磁盘基本 I/O 参数块，简称 BPB。BPB 中记录了有关磁盘的重要信息，如每扇字节数、每簇扇区数、磁盘介质说明等。BPB 最后的三个字，从位移 18H 开始，说明磁盘的每道扇区数、磁头个数和隐藏扇区数，它们是供给磁盘驱动程序使用的。

从引导扇区位移 21H 开始的 11 个字节为磁盘基数表。表中的各项参数与引导扇区中的 BPB 表及其它数据一道说明了整个磁盘的各种状态和使用情况。磁盘基数表主要供磁盘驱动器硬件操作时使用，它包括：磁头加载、卸载时间，马达等待时间，每扇区

字节数，扇区间隔字节数，等等。软盘基数表由磁盘I/O驱动程序INT 13H调用。

磁盘基数表的初始值固化在ROM－BIOS芯片的INT 13H程序中。它的入口地址是F000H:EFC7H。在上电初始化时，上电自测程序将其存放在中断向量1E中。在DOS启动过程中，DOS引导记录块修改1E向量，使它指向0000:0C21H，供DOS读盘操作使用。然后IBMDOS.COM模块的初始化程序再次修改1E向量，最终定位到0050:0070H，在此，由DOS建立新的磁盘基数表。

引导扇区中的BPB表及磁盘基数表中各字节的含义如表2.2所示，表中介质符的含义见表2.3。

表2.2　BPB表及磁盘基数表中各字节的含义

位移	字节	含　义	双面软盘内容	高密软盘内容
00H	3	JMP到引导程序	JMP 012E	JMP 012E
03H	8	OEM名和版本号	IBM 2.0	IBM 3.3
0BH	2	每个扇区的字节数	0200H	0200H
0DH	1	每个簇扇区数	02H	01H
0EH	2	保留扇区数(从0开始)	0001H	0001H
10H	1	FAT的个数	02H	02H
11H	2	根目录项的个数	0070H	00E0H
13H	2	扇区总数(含引导扇区、目录等)	02D0H	0960H
15H	1	介质符	FDH	F9H
16H	2	每一个FAT所占扇区数	0002H	0007H
18H	2	每一磁道的扇区数	0009H	000FH
1AH	2	磁头(面)个数	0002H	0002H
1CH	2	隐藏扇区个数	0000H	0000H
1EH	2	存放计算的驱动器号、磁头号		
20H	1	IBMBIO.COM文件所占扇区数	OAH	OAH
21H	1	高4位为步进速率，低4位为磁头卸载时间	DFH	EFH
22H	1	高7位为磁头加载时间，低1位为置DMA方式	02H	1AH
23H	1	马达等待时间	25H	25H

续表

位移	字节	含　义	双面软盘内容	高密软盘内容
24H	1	每扇区字节数(参量 0,1,2,3)	02H	02H
25H	1	每道扇区数	09H	0FH
26H	1	扇区间隔字节数	2AH	1AH
27H	1	每扇区字节数(当 3 字节参量为 0 时)	FFH	FFH
28H	1	格式化时扇区间隔的填充字节	50H	50H
29H	1	格式化时扇区数据的填充字节	F6H	F6H
2AH	1	寻道后磁头的稳定时间	0FH	00H
2BH	1	命令等待时间	02H	02H
2CH	2	重新引导	INT19H	INT19H

表 2.3　MD—介质描述符

十六进制	说　明
F8H	硬盘(17 扇区/道)
F9H	双面 5.25 英寸高密度软盘(15 扇区) 双面 3.5 英寸软盘
FAH	RAM 虚拟盘
FCH	单面 5.25 英寸软盘(9 扇区/道)
FDH	双面 8 英寸软盘(单密度) 双面 5.25 英寸软盘(9 扇区/道)
FEH	单面 5.25 英寸软盘(8 扇区/道) 单面 8 英寸软盘(单密度) 单面 8 英寸软盘(双密度)
FFH	双面 5.25 英寸软盘(8 扇区/道)

DOS 的引导程序和 DOS 的版本有关,但是无论版本如何,DOS 引导区的作用都是相同的,这些将在本章的 DOS 操作系统中给予详细说明。

2. 文件分配表(FAT 表)

文件分配表从逻辑 1 扇区开始,它存放每个文件在磁盘上分布的信息。文件分配表

是DOS的一个重要的数据表格。它可以用来登记文件区中所有磁盘簇号的分配使用情况，同时，可由文件的首簇号，在FAT表中快速地查找此文件链簇中其它簇号以及链接关系。

磁盘上共有两个完全相同的文件分配表，FAT1和FAT2。FAT2是FAT1的备份，是为了防止FAT1被破坏而专门设置的。

3. 根目录表(RDT表)。

RDT表记录根目录下每一个磁盘文件名、扩展名、生成时间和文件长度等等。

4. 数据区(Data Area)。

除了上述3个区外，磁盘剩余的空间，都用来存储程序和数据，称作数据区。

← DOS区 ——— →				←数据区
0	1　2	3　4	5～11	12——
引导记录区	FAT1	FAT2	根目录区	DATA　AREA

§2.2 硬　盘

2.2.1 硬盘的结构

硬盘和软盘一样，都是个人计算机常用的外存储器。但硬盘比软盘容量大，速度快。硬盘由多个盘片组成。PC机的硬盘一般由两个盘片组成，因而有4个磁头，编号为0到3。4个磁头对应的4个面为0面到3面。

硬盘的磁盘表面也以转轴中心为原点，均匀地划分为若干个半径不等的同心圆，叫做磁道。不同面上的相同半径的磁道，在垂直方向上构成的圆筒，叫做柱面。显然，柱面数等于磁道数。10MB的硬盘共有306个柱面，编号由外向内为0到305。20MB的硬盘有614个柱面，编号由外向内为0到613。1个面上每个磁道17个扇区，每个扇区(无论弧长大小)都存贮512个字节，所以对于10MB硬盘，全部字节数为：

$512\times17\times4\times305=10618880\approx1M$ 字节。

硬盘中的305柱面留作诊断用。

硬盘的物理扇区是磁盘扇区的绝对地址。物理扇区由驱动器号，磁头号(即面号)，柱面号和扇区号四个参数组成，如10MB硬盘的第一个物理扇区为03驱动器(C驱)0磁头0柱面1扇区。最后一个扇区是03驱动器3磁头305柱面17扇区。

硬盘的逻辑扇区与DOS分区的起点有关。DOS 3.0以下版本分区的硬盘只有1个系统隐藏扇区，DOS分区的起点由0磁头0柱面2扇区开始。DOS 3.0以上的版本有17个系统隐藏扇区，DOS分区从0磁头0柱面1扇区开始，由此可见，硬盘的逻辑扇区与物理扇区的对应关系因DOS版本的不同而不同。

2.2.2 硬盘的数据组织

硬盘可以划分为几个“分区”，用以支持 DOS 以外的操作系统。DOS 3.2 以下的系统，硬盘最多可容纳 4 个分区。每个分区可以具有不同大小的存储空间，但每个分区分配的存储空间都是连续的。因此在硬盘上可驻留 DOS，CP/M，UNIX 及其它操作系统。每一个操作系统都可以在硬盘上建立自己专用的操作区，但不能对盘上的其它分区进行操作；而且，在某段时间内，只允许盘上的一个操作系统运行。也就是说，几个操作系统不能同时运行。

每一种操作系统在硬盘上建立分区操作时都由一个自己特有的实用程序来完成。DOS 分区的实用程序为 FDISK.COM。利用 FDISK 可进行 DOS 分区的生成、删除、显示和修改等操作。

硬盘初始化时，可根据用户选择的地址和大小建立一个或几个用于 DOS 的区域。经过分区后，在硬盘上就建立了一个硬盘的主引导区和几个分区。

2.2.3 主引导扇区

硬盘的主引导扇区位于硬盘的 0 磁头 0 柱面 1 扇区，是硬盘上第一个物理扇区，主引导扇区中存放着硬盘的主引导记录。硬盘的主引导记录包括了 3 个方面的内容：主引导程序代码，分区表和主引导记录结束标志。

1. 主引导程序代码

主引导程序用来找出系统当前的活动分区，负责把对应的一个操作系统的引导记录即当前活动分区的引导记录，装入内存，然后把控制权转移给该分区的引导记录。

2. 分区表

主引导扇区的分区表存放在主引导记录的后半部分。分区表可分为 4 个部分(3.2 以下版本)，表示 4 个分区的信息，从位移量 1BEH 开始的 64 个字节是硬盘分区表，见表 2.4。

表 2.4 硬盘分区表

←—— 系统隐藏扇区 ——→		←——DOS 分区 I ——→				←—分区 II —→
主引导扇区	其它系统占用	DOS 引导扇区	FAT 区	目录区	数据区	

分区表的每一部分长 **16** 个字节，第 **0** 个字节是自举标志，该值为 **80H** 时，表示该分区是当前活动分区，可引导；当值为 **00H** 时，表示该分区不可引导。第 **4** 字节是 DOS 系统标志，其值为 **00H** 时表示不是 DOS 分区，值为 O1H 时表示该分区是 DOS 分区，使用 **12** 位文件分配表，值为 **04H** 时表示是 DOS 分区，并采用 **16** 位 FAT 表。分区表的第 **1—3** 字节是该分区的起始地址，其中第 **1** 字节为起始磁头号，第 **2** 字节的低 **6** 位为扇区号、高 **2** 位是柱面号的高 **2** 位，第 **3** 字节指出柱面号的低 **8** 位。因此，柱面号是用 **10**